Articles + Publications | February 14, 2024

That's a Wrap…or Not? Regulatory Data Incident Investigation Resolutions and the Path Forward

WRITTEN BY

Stephen C. Piepgrass | Samuel E. "Gene" Fishel | Sadia Mirza

This article was originally published on February 14, 2024 in Reuters and Westlaw Today. It is republished here with permission.

As we discussed in part three of this series, "Navigating the Complexities of Regulatory Data Incident Investigations," when an organization is the subject of regulatory data incident investigations, it must navigate a tangled regulatory web. Extricating itself from that web is the ultimate goal. But what form does that take?

Resolutions manifest through myriad permutations, but if the investigation does not resolve via litigation or settlement, the outcome can be frustratingly nebulous. Regardless, an organization's subsequent focus should be on compliance and avoiding the regulatory radar; thus, it should plan accordingly.

In the fourth and final installment of this series, we discuss the varied ways a data incident investigation concludes and how an organization can forge a successful path ahead in its aftermath.

Forms of Data Incident Investigation Resolutions

Depending on the size of the breach and the number of regulators involved, a data incident investigation can take years to resolve. State attorneys general, federal regulators, and state administrative agencies generally move very deliberately, and the more regulators involved the longer the investigation typically takes, particularly with larger incidents. Ultimately, such investigations will resolve through one of four ways: litigation, settlement, a closing notice, or silence.

Settlement

Investigations always risk developing into litigation that exposes organizations to potential court-imposed orders and judgments. Regulators may file court actions prior to negotiations or due to a breakdown in negotiations. Regardless of the order of events, data incident investigations often end in a negotiated settlement.

A settlement can take a variety of forms with different states, such as a Letter Agreement, Settlement Agreement, Assurance of Voluntary Compliance (AVC), Assurance of Discontinuance (AD), Consent Order, Consent Decree, Consent Judgment, or Stipulation of Judgment. Some regulatory agencies, especially on the federal side, have set forms through which they must resolve a case. State entities, however, vary widely, and the parties often may negotiate any of the above forms.

Whether a form is filed in court is dependent on each state's practices and procedures. Generally, Letter Agreements and Settlement Agreements are most often not filed in court, whereas AVCs and ADs likely will be filed in court, although not always. Consent Orders, Consent Decrees, Consent Judgments, and Stipulations of Judgment are almost always filed in court.

Whatever the form, agreements typically have two major components: injunctive relief and monetary relief. Regulators propose injunctive terms to improve organizations' security systems and related processes, and to enhance data protection and privacy measures. These terms could include, among other things, requiring segmentation or encryption of data, limiting access to databases, creating risk management teams, devoting a specific number of personnel to information security, adjusting how outside vendors are managed, or drafting more robust privacy policies.

Negotiations over injunctive relief can last for extended periods as organizations detail their current operations to regulators and regulators subsequently assess effective changes to implement.

Beyond reviewing company-specific goals, regulators also consider broader policy objectives when fashioning injunctive terms. This may include pushing an industry toward adopting newer, more comprehensive practices to avoid future similar incidents. A regulatory body will often highlight these developments through press releases following settlement. Organizations and associated counsel should therefore routinely monitor regulatory developments in this area to keep abreast of shifting parameters.

Monetary penalties, especially larger ones, offer regulators a higher-profile mechanism to advance their policy goals, as they are more likely to garner press attention and the attention of the broader industry. Regulators advocate for amounts that correspond to the perceived egregiousness of the incident, with higher amounts sought where there are large numbers of affected consumers involving more sensitive personal information.

While monetary payments are frequently punitive in nature, regulators also use monetary relief to signal to organizations to invest in robust data protection on the front end or pay on the back end. Settlements may also involve restitution for consumers when the incident has led to consumer loss, in addition to penalty amounts.

Finally, regulators typically insist on enforcement tools within an agreement, such as routine assessments where organizations report back to regulators at set intervals detailing compliance with settlement provisions.

Closing Notice and Silence

On rare occasions, a regulator will send a "close out" notice that they have closed the investigation and will take no action. Regulatory bodies often avoid such definitive statements because, although they are non-binding, they potentially expose the agency to public scrutiny if it later reopens the investigation because of new information or a change in administrations. Regulators thus prefer to reserve their rights by not "officially" closing a matter.

Sometimes frustratingly, a regulator may simply drop an investigation and never alert the subject organization of such. This is a common occurrence characteristic of data incident investigations. Regulators receive hundreds if not thousands of data incident reports every year, and their silence is often because of this deluge and the time it takes to officially "close out" inquiries by alerting every subject organization.

Additionally, there is no set time that must pass after an organization's last interaction with a regulator before it can assume an investigation is complete, which may be measured in years. Organizations must simply forge ahead despite this uncertainty with renewed vigilance and dedicated compliance in its cybersecurity and privacy efforts.

Forging a Successful Path Forward in an Investigation's Aftermath

Regardless of an investigation's outcome, an organization that controls or processes personal identifying information must comprehensively reassess cybersecurity measures, privacy policies, and incident response plans in its aftermath to identify gaps and take corresponding action to reduce the risk of future incidents and associated regulatory scrutiny.

Regulators assume that an organization under investigation has been put on notice and therefore should devote adequate resources to cybersecurity and privacy moving forward. Indeed, regulators have historically viewed organizations that suffer multiple incidents through a harsher lens.

While not an exhaustive list, below are some general measures that companies should consider to better position themselves should regulators ever come knocking:

- Regulators frequently request details about the security protocols and measures implemented prior to any incident. By establishing an information security program based on recognized frameworks like the CIS Security Controls or the NIST Cybersecurity Framework, organizations can demonstrate their proactive efforts to secure data. However, cybersecurity is not a one-time task; it necessitates ongoing monitoring and assessment of cybersecurity risks, and requires businesses to regularly review and update their security programs. It is worth nothing that the "reasonableness" of an organization's information security program depends on various factors, including the nature and volume of the data they handle or process. As a result, security measures that are deemed sufficient for one business may not be adequate for another. For instance, a small chain of smoothie shops processing only credit card numbers is not expected to invest in the same level of security resources as a tax service handling highly sensitive taxpayer information.

- Even the best cybersecurity measures and privacy policies can easily be circumvented if an organization does not adequately train its employees on best practices and company policies. Businesses should consider including not only instructional materials such as training videos, but also interactive exercises such as random "social engineering" tests that assess employees' vigilance. Methods such as fake "phishing" emails or "vishing" and "smishing" phone messages mirror current techniques that cybercriminals employ and provide illustrative examples for employees. Further, educating employees on how to identify and report security incidents through dedicated communication channels is equally important. Regulators often show interest in employee training, so investing time and resources in this area could yield significant benefits in the long run.

- Finally, tabletop exercises, which are simulated attacks designed to test an organization's ability to respond to a cyber incident, are also an effective way for an organization to measure preparedness. These exercises typically require the expertise of external professionals to run specific security incident scenarios, which can help organizations identify potential vulnerabilities and shortcomings in their existing plans. Tabletop exercises offer team members the chance to comprehend their roles and responsibilities during an incident, thereby

boosting their preparedness and confidence to manage real-world situations. They also promote collaboration and communication across various departments, enhancing overall coordination during an actual incident. Furthermore, these exercises may assist organizations in complying with regulatory requirements related to cybersecurity planning and preparation. For a tabletop exercise to be effective, it should involve decision-makers at all levels, from IT and security staff to C-suite executives and legal counsel. However, it's not necessary for all these individuals to participate simultaneously. Tabletop exercises are often divided into "technical" and "executive" sessions, reflecting the kind of incident response communications and collaborations an organization would encounter in reality.

Conclusion

A regulatory data incident investigation can follow several paths to conclusion, including through litigation or various forms of settlement. At times that conclusion may not be definitive as regulators may simply drop the investigation without further notice.

Regardless of the outcome, a regulatory investigation serves as a signal to an organization and as such it should endeavor to bolster its cybersecurity systems, privacy measures, and incident response plans. By investing in adequate resources and remaining vigilant of shifting threats and a changing legal landscape, an organization can avoid the worst fates of future potential investigations.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber